REMARKS

Applicants' claims have been amended to more clearly distinguish their invention from the art cited by the Examiner.

More specifically, each of the independent claims has been amended to recite that the inventive method allows secure communication from any sender to any recipient over a publicly-available network, such as the Internet; the communications are secure in the sense that an encrypted message is either capable of being decrypted only by an intended recipient, or in that a signature affixed thereto can be verified.

As discussed in the application as filed, the explosion of activity, particularly e-commerce, over the Internet has led to increased interest in secure communication and in signature verification. Various schemes to permit both are known. However, all of these of which the inventors are aware are intended to function only when the sender and recipient have the same encryption/decryption or signature verification software installed on their respective computers. The PTO e-filing plan exemplified by the Dickinson document cited herein is an example of this sort of scheme. The requirement of identical software for both sender and recipient sets up a significant barrier to the use of such schemes.

More specifically, using the conventional schemes, the user must do some or all of the following to enable secure communication:

Be aware of which cryptographic algorithms are executed
Find/negotiate/download/debug these algorithms
Manage cryptographic key relationships
Have a prior relationship or arrangement with the sending party

It will be appreciated that the Dickinson document requires all of these things of the user. While this may not be too much of a burden for a patent firm to shoulder, given that in theory it can be set up once and used many times thereafter, this is obviously much too complicated for use in routine e-commerce transactions between buyers of small items and their vendors.

According to the present invention these problems are overcome by incorporating the decoding or signature verification algorithm or a link thereto in the message itself. Then the secret key enabling decoding or signature verification need simply be separately communicated to the recipient, as is now also required. In this way any sender and any recipient can maintain secure communication in a simple and expeditious way over a public network. The claims define this invention clearly.

The art cited by the Examiner does not show or suggest this invention. Each of the three patent references relates to client/server secure communication, or similar high-level, non-public access. (See Jardin 6,671,810 at claim 1; Douglas 6,223,287 at the Abstract; and Finley 5,742,686, referring to host computer communication throughout.) It will be appreciated that it is much easier to see that a client machine has the same software as a server than to ensure that two strangers do so, and indeed the Jardin patent principally relied upon is directed to downloading particular software to a user. The claims have been amended in any event to further distinguish over the art by recitation that the method of the invention is useful between any sender and any recipient over a publicly-available network, as opposed to the dedicated client-server relationship discussed in these references.

It is therefore respectfully submitted that the claims as amended are in condition for allowance, and an early Office Action to that effect is earnestly solicited.

Respectfully submitted,

8/20/04
Dated

Michael de Angeli
Reg. No. 27,869
60 Intrepid Lane
Jamestown, RI 02835
401-423-3190